# Automating Logistics Support via a Wireless and Satellite Infrastructure

Author: Pat Summers, Sr. Systems Engineer, Raytheon Company, 1801 W. Hughes Drive, Fullerton, CA 92834 (714) 732-2115

Conference Session: "Designing Systems for Operational Security"

## ABSTRACT:

The purpose of this paper is to discuss a secure wireless global network approach to automate the logistics support for military aircraft maintainers. Currently, the aircraft maintenance personnel use out dated methods in tracking, tracing and reporting maintenance work order completions and the updating and the dissemination of related Interactive Electronic Technical Manuals (IETMs). Present day has the maintainer transporting select paper checklists, log sheets, equipment manuals and repair tools to the aircraft for maintenance by either truck or various carry on devices. The maintainer must then manually fill in paper checklists, work orders and completions and or computer logs for each assigned maintenance work orders and tasks. Then a Crew Chief or a responsible party must physically verify that the tasks have been completed before the aircraft is returned to service. The objective of this paper is to present an approach for a secure, reliable, paperless (Automate the Log, Tasks, Completion and Return to Service) system utilizing a user-friendly wireless network infrastructure. This local infrastructure can then be transitioned into the global support networks allowing for the dissemination of all types of real time critical and non-critical logistic based information on global squadron aircraft.

## Initial Concept

Maintainers will use a combination of interactive wireless devices that are part of an automated logistic environment. This environment includes seamless interfaces to (a) wireless LANs, (b) wearable heads-up Portable Maintenance Aids (PMAs) and (c) Personal Autonomic Logistic Systems (PALS). These highly functional devices allow the maintainer to have hands free, visual and voice contact within his maintenance zone and other team members while checking and maintaining all levels of logistics support for any designated aircraft. Each PALS unit will support wearable heads up applications, voice recognition, voice and video over IP. The improved IP telephony protocols and telecom equipment (e.g., application servers that leverage the transport capabilities of the data/voice/video network) will be incorporated in PALS units to increase system operational integrity and reliability.

Other Wireless Device Support Options:

- Bar code scanners identify specific aircraft parts;
  - 1D, 2D and 3D scanners
- Voice activation and recognition commands which will allow the maintainer to retrieve relevant data or video over IP switched data ports from central databases
- Memory Buttons for Data storage and Instantaneous reach back retrieval

This discussion reviews the issues, approaches, lessons learned, and evolving wireless IP equipment that must be considered to fully automate a global wireless systems approach in a highly distributed logistics support environment.

## INTRODUCTION:

Information is a critical resource in today's enterprises, whether it is military, industrial, commercial, or educational. Efficient accessibility to information and data is critical for effective and timely maintenance of commercial or military aircraft, or for any railway system. Currently the military aircraft maintenance work orders, log checklists, and completion logs generate volumes of paperwork. After the aircraft maintainer has completed all maintenance tasks, at a central repository, the paperwork must be organized, filed, and entered into the aircraft maintenance logs. This paper describes a high capacity infrastructure for providing wireless and broadband communication services to automate the logistics support for military, commercial aircraft maintainers or for railway maintainers. Automating the logistics maintenance process will eliminate the rigorous cumbersome paperwork and will provide state-of-the-art wireless access to the up-to-date maintenance manuals. In instituting a reliable seamless secure wireless network, security is a major issue. Security concerns and several potential solutions will be addressed. The goal of this paper is to describe the process to make the job of the aircraft or railway maintainer simpler, faster, more efficient, cost effective, reliable, and secure.

## MAINTENANCE CONCEPT AND DEPLOYMENT

### Deployment

The precision maintenance concept is to provide a world-class end-to-end interactive automated solution for the maintainer. Currently the Interactive Electronic Technical Manuals (IETMs) are large voluminous manuals that the maintainers refer to when maintaining military, industrial, commercial, or educational hardware. These paper IETM volumes are housed in maintainer warehouses. The maintainer must retrieve these IETM volumes from the maintainer warehouse prior to going on the flight line. Raytheon Technical Services Company (RTSC) has developed the Advanced Integrated Maintenance Support System (AIMSS) which is a Commercial Off The Shelf (COTS) IETM development and delivery system. The AIMSS authoring and distribution system offer a system that will create, maintain, and distribute powerful automated IETMs to the maintainer on the flight line via wireless interfaces. The IETMs authoring and distribution system has been designed to open architectural standards that will allow for future growth in software design, functionality, planning and decision aids for future Business Scenario development. See Figure 1 below.

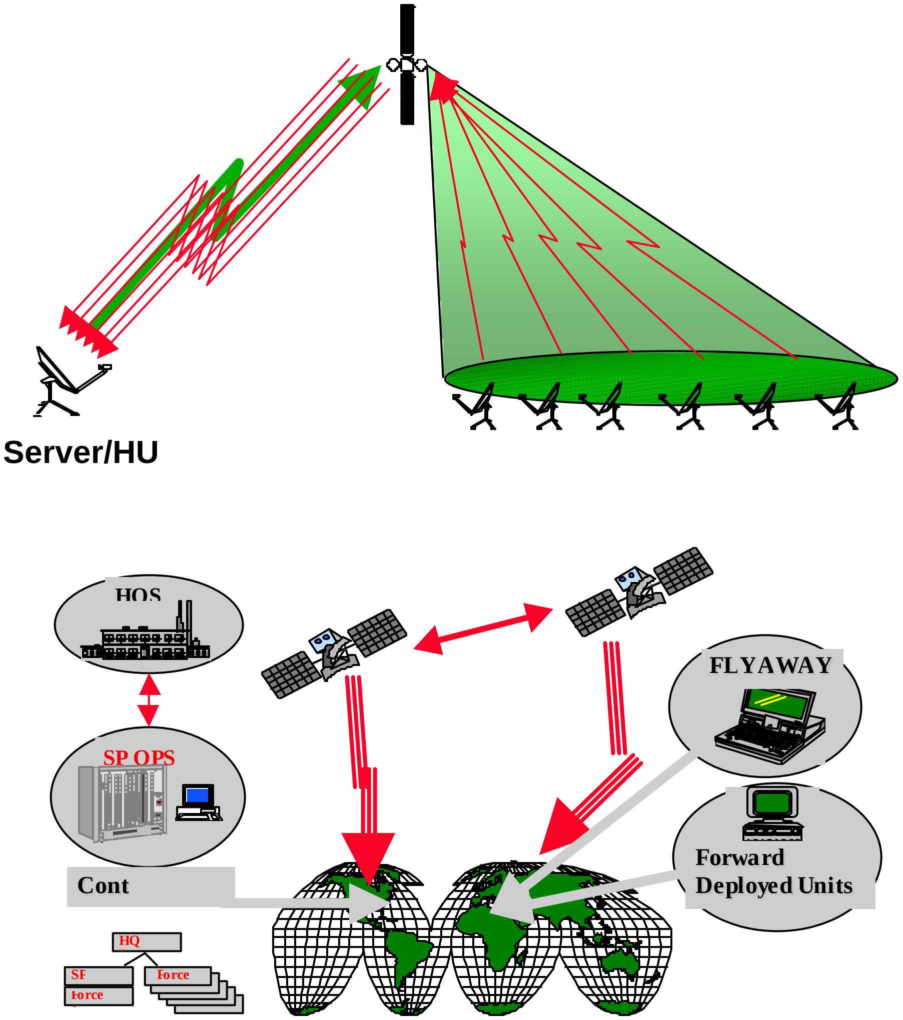

**Figure 1. Deployment Options**

The proposed infrastructure examined in this paper provides a solution for automating the logistics support for military aircraft maintainers (and their central database servers). This infrastructure is flexible and can interface to wireless video links, broadband systems (fixed broadband wireless > 10Mbps), wireless telephones, IP telephones, dataphones, direct broadcast satellites, digital assistants, portable networking (iPACs,etc.), LANs, WANs, and public switched telephone networks.  Figure 2 shows the platform devices and infrastructure.

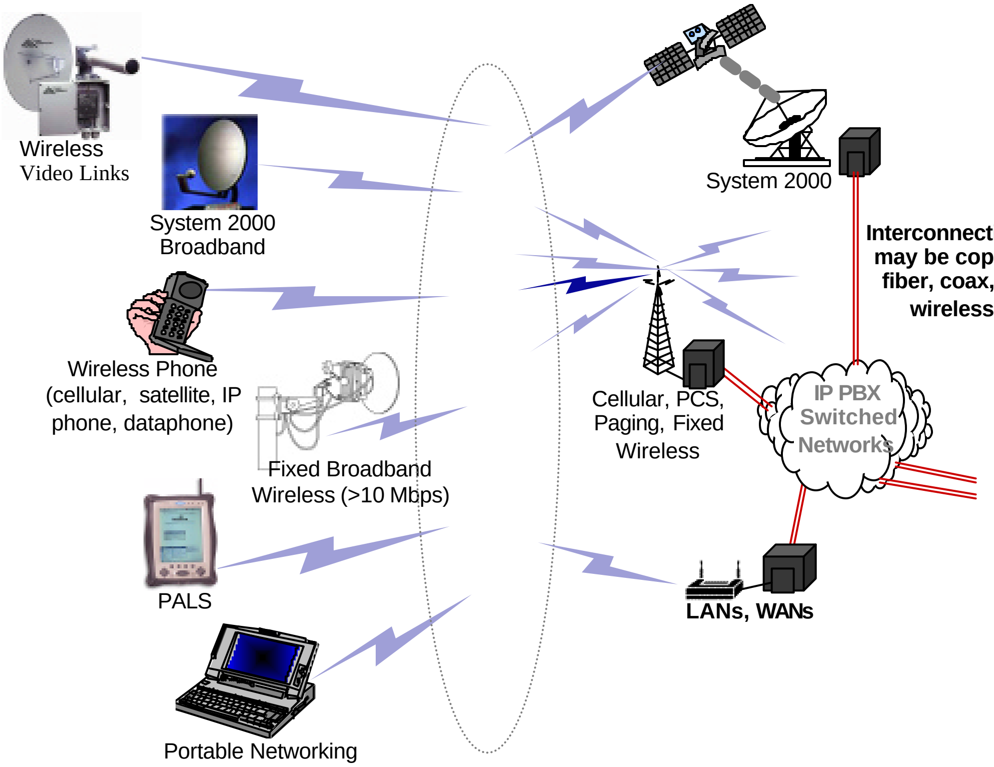

**Figure 2. Platform Devices and Infrastructure**

## ARCHITECTURE

The proposed infrastructure will provide a solution for automating the logistics support for military aircraft maintainers (and their central database servers) by transferring data, video, and voice over wireless connections, using voice activation commands which allow the maintainer to have total hands-free while performing maintenance. Since the maintainer is working using voice activation commands to page through the maintenance procedures/manuals (IETMs), this will expedite the maintenance process to evolve into a seamless paperless system.

Due to the inherent bottle-necks, reliability and performance issues associated with this architecture, a data centric distributed decentralized architecture has been designed. Distributed ground communication architecture ensures reliable, unambiguous, and accurate information distribution, data timeliness, data filtering and speed-of-service. Partially decentralized architecture, with at least one backup server, allows the processing load to be distributed among all the servers creating a completely collaborative structure. Decentralized architecture provides better performance reliability since you will not suffer from a single point of failure. Using a centralized hierarchical system architecture requires more bandwidth and is susceptible to performance throughput degradation and point of failure problems.

The wireless maintenance hardware can be easily implemented into the existing maintenance facilities with a 10/100 connection to an existing LAN/WAN. The servers and maintainer PDMAs are networked via a wireless network. The participating subnetwork zones are configured similarly except that each sunetwork zone has different zone subnetwork IP addresses. Maintaining modularity makes it easy for the network administrator to configure the network infrastructure and to monitor the network performance robustness and security. Figure 3 below shows a typical communication network of an existing LAN/WAN integrating seamlessly to wireless maintenance zones.

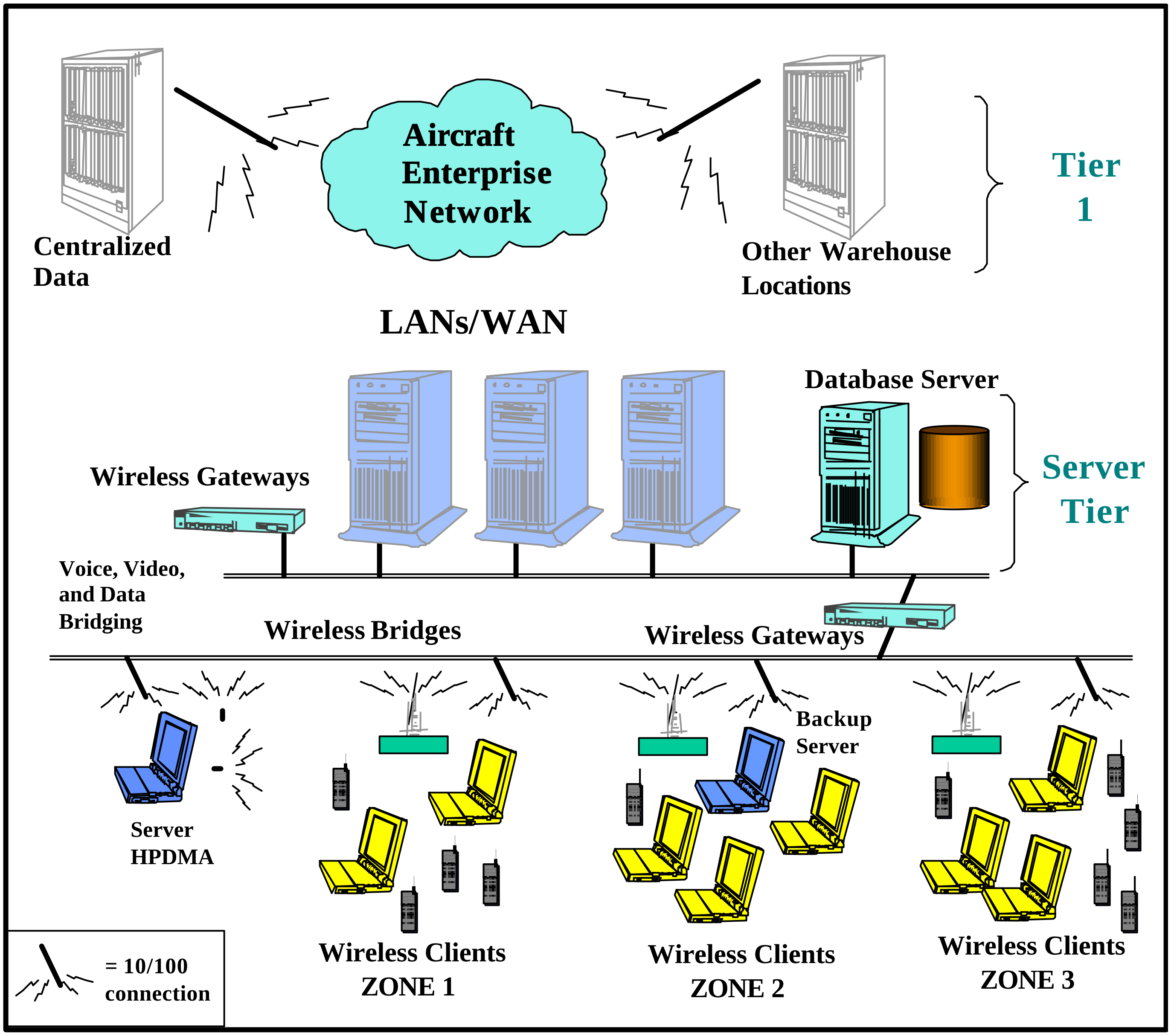

**Figure 3. Notional Communication Network**

Currently, the logistics maintenance process for the JSF, C130, F-18, and other military aircraft is a cumbersome activity with large volumes of Interactive Electronic Technical Manuals (IETMs) and limited or no automation.  Maintaining operability of the Aircraft is vital to its mission.  Having the technical manuals available during maintenance, inspection and checkout of the aircraft is essential to performing these tasks.  Storing these various maintenance publications in electronic format reduces the shear volume and logistics associated with hard copy manuals.  The aircraft maintenance personnel will no longer need to transport select paper checklists, log sheets, and bulky equipment maintenance manuals to the aircraft.  The aircraft maintainer will only need to take his personal heads-up wearable PDMA and boot up his personal computer, log on, identify himself, and scan the bar code on the aircraft in order to perform his maintenance tasks.  The specific maintenance procedures for the scanned aircraft part number will appear on his eyepiece display as well as a large display monitor, and the aircraft maintainer will be able to go through the procedure by verbally paging through the procedure and verbally going through the checklists and log sheets.  All the maintenance activity will be seamlessly automatically logged into the central database server for each maintenance activity that is performed.

For the wireless logistics solution on the military flight line (ground or sea), we are proposing a wireless network consisting of Access Points or a base station.  In this type of network, the Access Point acts like a hub providing connectivity for the wireless wearable computers.  This network can be connected or “bridged” to an existing wired LAN allowing the wireless computer access to LAN resources such as file servers, central databases, or existing internet connectivity.  Raytheon has a proprietary agreement with Symbol Technologies, one of the leading edge wireless manufacturers and the technology leader in bar code scanning processes.  Also, Raytheon has a proprietary agreement with Nortel Networks to participate in their Beta Program which allows Raytheon to test and validate the performance and functionality of the Meredian 11C IP PBX prior to public release.  By being a member of the Meredian Beta Program, Raytheon can make judicious recommendations to Nortel Networks for improving or enhancing the performance of the IP PBX prior to public release.  The IP PBX will allow access to any internal LAN or can easily be adaptable to interfacing to external networks via a Universal Trunk Card.

## IMPLEMENTATION

Institute a reliable network management scheme for several subnets at a site connected to the main server.

Implementing a wireless network required several studies to evaluate the various wireless manufacturer’s products.  Various hand held and wearable PDMAs were evaluated to determine the most efficient design when evaluating the various wireless vendor products for performance and reliability.  For ease of use, a wearable heads-up PDMA is recommended on the airfield flight line.  The wireless wearable mobile heads-up PDMA supports both an interface to a Symbol Technologies scanner and also accommodates voice activation commands for retrieval of information. Human Machine Interface (HMI) memory buttons may be an option for data storage and instantaneous reach-back retrieval of data or video from the maintainer database servers. Retrieved IETM information can be either data or video from the database server, and the field maintainer can be assured that the IETM retrieved from the maintainer warehouse is the most current version. The IETMs will be updated at all the central servers automatically via the satellite links at the same time. A monocle video display screen is attached to the wearable PDMA, but a backup ruggedized flat screen displays the same information as displayed on the monocle video display. Thus the maintainer is able to view and retrieve the data and diagrams from the IETM on a large scale.

The tracking maintenance for each aircraft or land vehicle will be seamlessly logged since all maintenance activity, checklists, data logging, and documentation will automatically be done for each maintainer and each aircraft via the wireless link. Thus, all paper checklists and log sheets will be eliminated. All maintenance activity, spares replaced, time spent by the maintainer, and all logging notes and anomalies will be automatically logged online to the main database servers. Using manual, voice activation commands, or a barcode scanner to retrieve information allows the maintainer to go to directly to a specific locations in the IETM and promotes a user-friendly automated retrieval of information via wireless links. Maintainers can manually enter keyboard strokes or use voice activation commands to retrieve both data and real-time video over IP information, in order to have hands-free to be able to work on any aircraft part unencumbered. Maintainers can also request real-time online help from an expert maintainer at the centralized distribution center server. The maintainer can then interact in real-time with the expert at the centralized database maintenance warehouse.

For optimum performance, reliability, and speed of service, the Frequency Hop Spread Spectrum (FHSS) Access Points will be implemented using the 802.11 protocol or prevailing standards as the primary waveform baseline for the wireless network infrastructure. Several independent subnets (access points with several PDMA subscribers) will operate independently and will be connected to the central database hub. Using the FHSS schema versus the Direct Sequencing Spread Spectrum (DSSS) schema provides inherently higher network security and reliability since the FHSS schema hops between 79 channels (2.4 to 2.4835 GHz) at a periodicity random access. The DSSS schema hops between 11 channels allocated to *x* number of users, and DSSS requires at least a 3 channel separation between users or RFI/EMI interference and data latencies will occur. With DSSS, overlapping zones will only create more contention for channel bandwidth and more data latencies and interference will be seen. Therefore, the FHSS spectrum jamming can only occur by full spectrum interference. To protect against interfering signals with finite power, the desired narrowband signal should be spread in a zoned user approach. A zoned user approach is recommended to allow multiple maintainers to work freely on more than one maintenance aircraft on a non-interfering RF basis. This will also add to higher inter system performance and give each of the zones its own privacy from other close-by wireless network activities.

Each maintenance subnet will be uniquely configured for each flight line maintenance station zone by assignment of unique IP addresses.. All subnets at the same airfield will be connected seamlessly to the central database server hub and will function independently without interference from the other flight line maintenance station zones. All central database servers will be updated regularly as the IETM manuals are updated. Therefore, all airfield central database servers will always have the most recent version of the aircraft IETM manuals to deploy to the maintainers.

Multiple access points can be connected to a wired LAN or sometimes to yet a second wireless LAN to accommodate additional flight line maintenance station zones. Access Points can be used as wireless relays, extending the range of a single Access Point. How? When a single network is too large to be covered by a single Access Point, then multiple Access Points can be used but the Access Points must overlap its neighboring Access Points and the network IP protocols must be set to match the same flight line maintenance station zone protocols. This provides a seamless area for users to move around in using a feature called “roaming”. “Roaming” allows the users on the airfield maintenance flight line to maintain a steady network connection by monitoring the signal strength from in-range Access Points.

## **SATELLITE COMMUNICATIONS**

Using satellite links to connect to the maintainer centralized data warehouses will ensure access data integrity with the wide-band multi-channel services. Satellite links are capable of using a combination of constellations and covering a wide area on land or at sea. Satellite links provide rapid deployment of IETM data, maintenance log history, test procedures, C3 backup, supply management, interactive training, medical consults, and moral communications. Real-time satellite links provide fail-safe performance. Satellite coverage is 24 hours a day, 7 days a week (24/7), and allows the network user/maintainer to have full access and support from the Conus-based cadre of technical experts by immediately connecting to the centralized maintainer warehouses.

### KA-BAND SATELLITE SYSTEMS

The explosion in communications, overcrowding of lower bands, and success of the NASA ACTS, ITALSAT and other international initiatives have provided the impetus for proposals for a large number of national, regional and global systems in Ka-band (30 GHz uplink/ 20 GHz downlink). The nature of the Ka band feed design lends itself to being expandable to more frequency ranges. The Ka band is beginning to be a requirement with many systems. The band feed design allows a straightforward expansion into KA band should the requirement arise to have a quad-band antenna system. The addition of the KA band requires the addition of a circular waveguide to the center of the Ku band waveguide. With this extension, the Ku band would be handled identically to the C- and X-band sections. The technique for combining a Ku band with a Ka band, creating a high frequency dual-band feed, could reduce the size of the reflector and provides a solution to the requirements for tri-band operation with potential for growth.

The Ka band had has very limited coverage due to the smaller antenna architecture. The Superbird covers Japan and the Astra covers Italy and a few other areas of Europe. Panamsat has spot beams on select cities in the United States.

Predominately, the Ku band satellites cover the majority of the land masses. The C-band covers most of the areas over water since the Ku band's performance is degraded over water due to the physical size and physical characteristics of the Ku band. The Ka band is environmentally friendly and more reliable than the Ku band in moist weather conditions. The frequency spectrum of the C-band, Ku-band, Ka-band and L/S is shown in Table 1 below.

| **BAND** | **UP-LINK (GHz)** | **DOWN-LINK (GHz)** | **ISSUES** |
|---|---|---|---|
| C | 3.7 - 4.2 | 5.925 - 6.425 | Interference with ground links |
| KU | 11.7 – 12.2 | 14.0 – 14.5 | Attenuation due to rain |
| KA | 17.7 – 21.7 | 27.5 – 30.5 | High equipment costs |
| L/S | 1.610 – 1.625 | 2.483 – 2.500 | Interference with ISM band |

**Table 1. Frequency spectrum allocation for common commercial SATCOM bands**

All communication channels and video links are conditioned to common CCITT standards. Links will support both simplex and duplex communications. Links are protected from RF power loads by automatic transponder shutdown. Standard EIA-530 are used for modem interfaces with cryptographic and data processing equipment. Data modems have fallback capabilities during link degradation. All users and maintainers are ensured a 95% first-time success rate and link availability at 99.9%. All satellite links are reconfigurable by a dedicated operation control center. In the case of OCONUS control, these links are controlled by CONUS/OCONUS gateways.

## NETWORK PRIVACY AND SECURITY

Security addresses confidentiality and prevention of compromise of sensitive/classified data. The integrity of the IETMs must be maintained and unauthorized modification of the IETM data must be prevented. Security must be able to detect any unauthorized users, compromise of network security, compromise of computer security, any transmission or encryption tampering or interference, or any infrastructure network attacks on the availability of critical system services. Any unauthorized threats: 1) connections to the internet, the Secret Internet Protocol Router Network (SIPRNET), and Non-Classified IP router Network (NIPRNET); 2) unauthorized users within the maintenance centralized data maintenance warehouses; and 3) unauthorized users outside the data maintenance warehouses, should be capable of being detected. The security architecture must be configured to identify and authorize all user clients/maintainers at the points to be protected, and this must be reinforced with a security "behavior model" that will trigger a state transition when an intruder is detected. This "behavior model" would need to capture any information that the intruder is testing or attempting to access in the database, and multi-level security must be integrated into the wireless architecture to ensure network and accuracy and integrity.  Filters, firewalls, guards, security intrusion detection tools, security management tools, encryption, and Netlock management tools must be capable of detecting any unusual or unauthorized activity on the network, and must be able to shut the intruder down before network performance and integrity is compromised.

Recently security breaches in the 802.11 standards have identified the need for more network protection.  The IEEE 802.11 standard specifies a security method called Wired Equivalent Privacy (WEP) protocol that was designated RC4, encrypts the message with a 40-bit security key or a 128-bit security key, which may also be compromised.

For smaller networks, an "Out-of-the-Box" set of solutions may be a small tightly managed Virtual Private Network (VPN).  First, all servers and client maintainers PDMAs will have network monitoring intrusion software capabilities, an automated agent personal client network protection system.  This approach is fully scalable to 802.11 clients and has low administration requirements.  Each VPN server can be centrally administered and traffic to the internal wireless Access Points (AP) zones is isolated until VPN authentication is performed.  "Netlock" works at the operating system network layer, below the transport layer of TCP/IP and the IPX protocols.  Netlock implements the IETF IP Security (IPSec) for the TCP/IP and the IPX/SPX protocols.

"Netlock"comprises a suite of software four software modules:

- Netlock Manager that is installed on the network or the maintainer warehouse's servers, enabling him to define and maintain security policies from a central location.  Encryption and authentication algorithms are included here.
- Netlock Agents are installed on all the user maintainer PDMAs or computers on the secure network.  The Network Manager sends the Network Agents the security policies for local storage, and the Network Agents follow the security policies autonomously when communicating on the network.
- Netlock Gateways may be included to provide secure communications between Network Agents and other network entities.
- Netlock Auditor is optional and may be included in the network to provide a third-part administrator, such as an ISP, the ability to review an administrator's changes and to ensure that any changes were made correctly.

Additionally Raytheon has a proprietary agreement with Symbol Technologies, Symbol Technologies has offered to assist in the implementation of the Kerberos File Key security (secure data with 128 bit encryption).  The Kerberos FileKey security will allow secure C2 data to be transmitted over these independent networks.

Single DES and triple DES (3des) are the most common cryptographic algorithms currently in use.    SKIPJACK is a relatively new encryption algorithm and has not received as much scrutiny as the DES 64-bit block, 56-bit key cipher algorithm. SKIPJACK also uses the 64-bit block, but it uses 32 rounds which is twice as many as DES uses. Because SKIPJACK is constructed of simpler operations, it actually runs about twice as fast as DES, and SKIPJACK does not require any set up time. The DES encryption algorithms have also been compromised.

To provide security to users/clients/maintainers, the 3DES file encryption algorithm integrated with secure hardware can provide a high-level of baseline network stability and intrusion protection. As the PCs, microprocessors, and the hardware speeds increase, it is becoming inherently more difficult to provide network and system security using only cryptographic algorithms. Variations of the encryption algorithms and unique hardware system designs must continue to develop and mature to ensure the integrity of data networks and databases.

The Fortezza crypto card is a hardware-based security token that is a major component of the Multilevel Information Systems Security Initiative (MISSI) Program. The MISSI program's goal is to distribute an evolving set of solutions that provide secure interoperability in a network security framework based on common security standards and protocols. The Fortezza hardware cryptographic card provides security services such as data confidentiality, user authentication and data integrity. Fortezza's encryption capabilities restrict unwanted access to the network from unauthorized clients/maintainers or the servers. Currently, several Beta Test Sites and Secure Computing Corporation are developing hardware and software prototypes to provide security for SECRET and TOP SECRET networks and databases. MISSI will need to define the organizational policies, structure, and procedures prior to the implementation of the Fortezza encryption cards into the secure networks.

For protecting sensitive data in United States government voice and data networks, the National Security Agency (NSA) controls which algorithms are exportable outside the U.S.

## FUTURE WIRELESS BROADBAND PROJECTIONS

### What next?

According to International Data Corp., June 26, 2001, "Small displays, slow transmission speeds and cumbersome data-entry methods will limit mobile Internet usage to functions that are dependent on timing, location, or experience. While these traits work well with a select group of transactions (such as last-minute travel changes), the vast majority of usage will inevitably be information query. Because of their time or location sensitivity, e-mail, stock quotes, weather, travel delays and itineraries, and point-to-point directions are expected to be among the most commonly accessed mobile Internet services. Although these services do not represent direct commerce opportunities, they will be leveraged by e-businesses to help build customer relationships and open the door for indirect commerce."

Implementing a wireless network required several studies to evaluate the various wireless manufacturer's products. Currently the existing heavy and bulky wearable mobile heads-up PDMA must be interfaced to a separate scanner. The future wearable mobile heads-up PDMA will be smaller and weigh less. The future PDMA will have a Symbol Technologies scanner incorporated into the hand held PDMA, and the same PDMA will accommodate voice commands and will display data and/or streaming video. The design may incorporate small eyeglasses or a single monocle video display screen connected via a wireless connection to the wearable PDMA, but a backup ruggedized flat screen displays the same information as displayed on the monocle video display. The evolving future wireless wearable mobile heads-up PDMAs are becoming smaller, weigh less, have faster processors, have better video monocles, and will have a more user-friendly speech recognition software package.

The fixed broadband wireless systems LMDS (local multipoint distribution service) access is not cost effective since the IEEE 802.11 (a-k) standards vary from version a through version k. The IEEE has formed a task group to bring standardization to the broadband wireless sector, and they have dubbed it as 802.16.1, 802.16.2, and 802.16.3. Table 2 below shows defines the 802.16 wireless standards.

| NAME | WHEN PUBLISHED | RANGE/ DETAILS |
|---|---|---|
| 802.11 | 1997 | Operates in a 2.4 GHz range, same as cordless phones |
| 802.11.b | 1999 | Operates in a 2.4 GHz range. This is the standard used by most corporate wireless LANs today. Offers data rates of up to 11 Mbps. |
| 802.11.a | 19999 | Operates in a 5 GHz range. Offers less distance capability between base station and client(s). Proposes to offer data rates of up to 54 Mbps. |
| 802.11.e | In development | Will provide enhanced voice transmission and enhanced security features such as larger encryption keys and 128-bit encryption |
| 802.11.g | In development | Operates in a 2.4 GHz range. |
| 802.16.1 | In development | Defines the air interface for 10 to 66 GHz systems (defines the interface between the subscriber's transceiver station and the base transceiver station) |
| 802.16.2 | In development | Covers coexistence of broadband wireless access systems (such as voice and ATM, over the air interfaces) |
| 802.16.3 | In development | Defines the air interface for licensed systems operating in the 2 to 11 GHz band (defines the repeater and reflector interfaces to wireless systems) |

*NOTE: 802.1.6.x specification data extracted from "Communications System Design", (September, 2001), pages 38-46.

**Table 2. Wireless Standards**

The IEEE 802.11 (a-g) protocol standards are well publicized and have documented standards; however, each of the 802.11.a through 802.11.g protocols needed some standardization. The IEEE 802.16.x standards are not well known, but it appears that the 802.16.x protocols will eventually become the broadband wireless standard, so the next few paragraphs will described the IEEE 802.16.x protocols.

The requirements for the 802.16 standard are defined in terms of support bearer services. For example, an 802.16 interface must be capable of supporting the data rate and QoS required by an ATM network or an IP based network. The 802.16 interface must also be able to support the data rate and delay requirements of voice or video transmissions.

The four protocol layers defined in the 802.16 protocol architecture are the Convergence and Media Access Control (MAC) layers of the OSI data link layer and the Transmission and Physical (PHY) layers of the OSI physical layers. The MAC layer protocol defines how and when a user/maintainer may initiate transmission on the channel. Since the ATM requires specified service levels such as QoS, the protocol must be able to allocate radio channel capacity to satisfy service demands. On top of the MAC layer, the specification contains a Convergence layer that provides functions specific to the services being provided such as: 1) encapsulating Protocol Data Unit (PDU) framing of upper layers into the native 802.16 MAC/PHY frames; 2) map an upper layer's addresses into 802.16 addresses; 3) translate upper layer QoS parameters into native 802.16 MAC format; or 4) adapt the time dependencies of the upper layer traffic into the equivalent MAC service.

The 802.16.1, air interface data transmissions are structured as a sequence of MAC frames. The 802.16.1 PHY supports a different structure for the point to multipoint downstream channels and the multipoint to point upstream channels. Upstream transmission uses a Demand Assignment Multiple Access (DAMA)-TDMA technique. With DAMA-TDMA, the assignment of slots to channels varies dynamically. In the downstream direction, there are two standard modes of operation: 1) Mode A - continuous transmission stream; and 2) Mode B – burst transmission stream such as IP-based traffic.

## **FUTURE INTEREST**

Mobile wireless devices and new innovative wireless concepts will drive the growth of the Wireless LAN market in the Air Force, Navy, Marines, Army and commercial aircraft industry. The future of wireless technology and wireless concepts is maturing and evolving rapidly. The future of smaller PDMA (e.g.: A Palm VII or iPAC with an IR link to a laptop) and wearable PDMAs with faster and smaller wireless hardware allows efficient reliable data, voice, and video transmissions to occur simultaneously on adjacent separate networks accessing common resources (servers, databases, etc.). Worldwide network connectivity to common databases and centralized data warehouses via satellite broadband coverage provides redundant global support. Multiple aircraft can share reliable data and voice resources while roaming seamlessly amongst the outdoor networks. Many security features and redundancy ensure that only authorized users can efficiently access their assigned aircraft networks with no interference from the adjacent and surrounding networks and subnetworks.

Raytheon is currently working as a Boeing team member on the Joint Strike Fighter (JSF) Program. Raytheon will provide the architecture and recommend the ground portal interfaces for the wireless networks based on the JSF wireless maintenance and ground/ship communications requirements. Raytheon will support Ground to Air, Air to Ground Portal Network design and wireless zone network relays. Both 2D and 3D wireless automated bar code scanning and IP voice over wireless zones will be implemented. GUI and middleware will be designed and installed to ensure a user friendly system. The JSF security requirements will be evaluated and appropriate software and hardware solutions will be provided to ensure a fail-safe reliable seamless wireless network.

The Air Force Research Laboratory (AFRL) has worked with the Raytheon facility in Fullerton, California and been identified as a technology center of excellence. for an informal wireless briefing. AFRL is also interested in implementing wireless networks into several Air Force applications. Raytheon proposes to perform wireless zone network evaluations and throughput estimates as well as network modeling and simulation to ensure an efficient robust logistics system at the various airfields.

Venntronix, an Army contractor from Fort Monmouth, New Jersey, is also interested in adding the uses of wireless for satellite and ground communications to their Junior Military Training Curriculum. They have expressed interest in our wireless study of the wireless equipment and implementation and they may ask Raytheon to be an integral team member in coordinating and generating the wireless training curriculum viewgraphs.

Other military and Government agencies have expressed interest in implementing state-of-the-art wireless networks in their facilities for various applications. With the rapidly evolving wireless technology becoming lighter, smaller, having higher throughputs and greater range with more robust communications, the ease-of-deployment is making the use of wireless becoming more attractive to commercial as well as other Government users.

Wireless communications using voice recognition software is becoming more sophisticated and more complimentary with PC based networks, therefore making it more user-friendly and allowing the user to dictate data and information versus writing the information. Wireless communications are being used in more households for networking and data access, just as the PCs were prevalent in the 1980s. As wireless and satellite technology is ever evolving and maturing, the rapid deployment of IETMs, databases, network hardware or software enhancements/upgrades must be addressed. In the logistics world, the AIMSS

IETMs can be accessed via the Wide Area Network (WAN), AIMSS web-enabled run-time viewer, and the databases can be accessed via the Windows Internet Explorer.

## SUMMARY / CONCLUSION

Automating logistics maintenance will save time, labor, and costs. Creating a seamless wireless network will save time, reduce the number of maintainers, reduce the false removal of system components, reduce the spares costs, will automate the paper process (log sheets and checklist sheets), and can be applied or adapted to many existing systems with no or minimal hardware changes. With the satellite link technology and reliability evolving and maturing, the world wide satellite access, performance and coverage is also improving. The wireless technology and transmission protocols are constantly evolving and creating new standards such as the IEEE 802.16 protocols. Wireless security issues must be addressed and configured for every unique system to ensure bulletproof layers of security since the existing WEP security protection is capable of being compromised. Both existing encryption hardware and software cryptographic algorithms must be developed, modified and integrated to ensure reliable fail-safe data and network infrastructures.